UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/043,426	01/10/2002	Jeff B. Anderson	01545.018c	9046

7590   03/18/2005

Daniel P. McCarthy
PARSONS, BEHLE & LATIMER
201 South Main Street, Suite 1800
P.O. Box 45898
Salt Lake City, UT 84145-0898

EXAMINER
REILLY, SEAN M

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Office Action Summary	Application No.	Applicant(s)
		10/043,426	ANDERSON ET AL.
		Examiner	Art Unit
		Sean Reilly	2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

This office action is a first action on the merits of this application. Claims 1-29 are

presented for further examination.

Priority

1.   The effective filing date for the subject matter defined in the pending claims in this

application is 1/10/2001.

Specification

2.   The abstract of the disclosure is objected to because it exceeds the 150-word limit.

Correction is required. See MPEP § 608.01(b).

3.   The specification is objected to for not cross-referencing co-pending applications 10/044632

and 10/044114 in the section entitled CROSS-REFERENCE TO RELATED APPLICATIONS.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine

grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

improper timewise extension of the "right to exclude" granted by a patent and to prevent possible

harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.

Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686

F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA

1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to

overcome an actual or provisional rejection based on a nonstatutory double patenting ground

provided the conflicting application or patent is shown to be commonly owned with this

application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal

disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37

CFR 3.73(b).

4.   Claims 1-29 are provisionally rejected under the judicially created doctrine of obviousness-

type double patenting as being unpatentable over claims 1-21 of copending Application No.

10/044632. Although the conflicting claims are not identical, they are not patentably distinct

from each other. Refer to the tables and remarks below for specific claim mappings and further

explanation.

5.   Claims 1-29 are provisionally rejected under the judicially created doctrine of obviousness-

type double patenting as being unpatentable over claims 1-35 of copending Application No.

10/044114. Although the conflicting claims are not identical, they are not patentably distinct

from each other. Refer to the tables and remarks below for specific claim mappings and further

explanation.

6.   This is a provisional obviousness-type double patenting rejection because the conflicting

claims have not in fact been patented.

7.   In the instant application, claim 26 substantially incorporates the limitations of independent

claims 1, 11, 20, 21, and 22. Similarly claim 17 of application 10/044632 substantially

incorporates the limitations of independent claims 1, 5, 9, 10, 11; and claim 35 of application

10/044114 substantially incorporates the limitations of independent claims 1 and 29. Thus, the

limitations of claim 26 in the instant application are mapped to the limitations of claim 17

application 10/044632 and claim 35 application 10/044114 to form the basis for the double

patenting rejection.

8.   Claim 26 of the instant application is method for remotely accessing and viewing information

about an enterprise, while claims 35 and 17 of the co-pending application are directed to systems

for executing such a method. The method steps of claim 26 include: accessing a transferential

system, utilizing the transferential system to access an enterprise, and utilizing the transferential

system to view information about the status and operation of the enterprise and its components.

In order to use the systems of the co-pending applications for their claimed functionality the

method steps of claim 26 must be executed, thus the co-pending claims are not patentably

distinct.

Instant Application # 10/043426	Co-pending Application # 10/044114 Claim 35
26. A method for remotely accessing and viewing information about an enterprise, comprising the steps of:	35. A reporting and maintenance system for remotely monitoring or controlling devices in an enterprise, comprising:
accessing a transferential system that has the following characteristics:	
a server group including at least two servers, said servers providing redundancy of	a server group including at least two servers, said servers providing redundancy of

operation, at least one non-volatile memory device incorporated to said server group,	operation; at least one non-volatile memory device incorporated to said server group;
server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity,	server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity;
1-10 computer readable instructions	1-10 computer readable instructions
a cabinet housing said server group, a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet, a second network enabled temperature sensor, said second temperature sensor	a cabinet housing said server group; a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network enabled temperature sensor, said second temperature sensor

positioned to monitor the temperature of the air outside said cabinet, at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position, locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a superintendent system, a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device, a network enabled camera whereby a space in proximity to said server group may be monitored, an alarm in proximity to said server group, a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands	positioned to monitor the temperature of the air outside said cabinet; at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a superintendent system; a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device; a network enabled camera whereby a space in proximity to said server group may be monitored; an alarm in proximity to said server group; a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands

from a superintendent system,	from a superintendent system;

Instant Application # 10/043426	Co-pending Application # 10/044632 Claim 17
26. A method for remotely accessing and viewing information about an enterprise, comprising the steps of:	17. A transferential system for remotely monitoring or controlling devices in an enterprise, comprising:
accessing a transferential system that has the following characteristics:	
a server group including at least two servers, said servers providing redundancy of operation, at least one non-volatile memory device incorporated to said server group,	a server group including at least two servers, said servers providing redundancy of operation; at least one non-volatile memory device incorporated to said server group;
See enterprise device in communicative proximity below	enterprise devices in electronic communication with said server group through said server network hardware;
See superintendent system below	a central information system in electronic communication with said server group through said server network hardware;
server network hardware connected to said	server network hardware connected to said

server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system **(central information system)** through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity,	server group, said server network hardware including a gateway, said server network hardware providing encrypted electronic communication between said server group and said central information system through said gateway, said server network hardware further providing electronic communication between said server group and said enterprise devices;
see first computer readable instructions which starts the notification process; superintendent system monitor displaying messages	at least one notification device connected to and controllable by said central information system whereby an administrator may be notified of enterprise status; at least one display device connected to said central information system providing display facilities to administrators;
1-10 computer readable instructions	1-10 computer readable instructions
a cabinet housing said server group, a first network enabled temperature sensor, said first temperature sensor positioned to monitor the	a cabinet housing said server group; a first network enabled temperature sensor, said first temperature sensor positioned to monitor the

temperature of the air at the interior of said	temperature of the air at the interior of said
cabinet, a second network enabled temperature	cabinet; a second network enabled temperature
sensor, said second temperature sensor	sensor, said second temperature sensor
positioned to monitor the temperature of the air	positioned to monitor the temperature of the air
outside said cabinet, at least one door included	outside said cabinet; at least one door included
in said cabinet whereby access to said server	in said cabinet whereby access to said server
group is restricted when said doors are in	group is restricted when said doors are in
closed position, locks included in said doors	closed position; locks included in said doors
whereby said doors may be secured in a closed	whereby said doors may be secured in a closed
position, said locks enabled to unlock through	position, said locks enabled to unlock through
an electronic command message from a	an electronic command message from a central
superintendent system, a data entry device	information system; a data entry device
connected to said locks, said data entry device	connected to said locks, said data entry device
being mounted to said cabinet, said data entry	being mounted to said cabinet, said data entry
device providing a human interface external to	device providing a human interface external to
the cabinet enclosure; said locks enabled to be	the cabinet enclosure; said locks enabled to be
unlocked through said data entry device, a	unlocked through said data entry device; an
network enabled camera whereby a space in	alarm in proximity to said server group; a
proximity to said server group may be	network enabled power controller connected to
monitored, an alarm in proximity to said server	and being configurable to control the power of
group, a network enabled power controller	at least one server of said server group, said
connected to and being configurable to control	power controller being configurable to accept

the power of at least one server of said server group, said power controller being configurable to accept network commands from a superintendent system,	network commands from a central information system;

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9.   Claims 9, 16, 19, 22 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Regarding claims 9 and 19, the limitation "a notification channel protocol" renders the claim ambiguous. The definition of a notification channel protocol is not known in the art. It is presumed the applicant indented to recite the limitation "a notification protocol" which is defined on pg 2 ¶ 29 lines 1-3 of the specification.

11. Claim 16 recites the limitation "said receiving of second device status messages" in line 3. There is insufficient antecedent basis for this limitation in the claim.

12. Regarding claim 16, the claim as written is ambiguous. It is not clear what "said receiving of second device status messages" refers to. It is presumed the applicant intended claim 16 to similarly read as claim 6.

13. Regarding claims 22 and 26, the claims as written are ambiguous. The limitations "enterprise devices in electronic communication with said server group through said server

network hardware" and "a superintendent system in electronic communication with said server

group through said server network hardware" at the bottom of pages 35 and 38 fail to further

limit the claim since such limitations are already present in the claim, see pgs 34 and 26 the

limitations "a superintendent system" and "at least one enterprise device in communicative

proximity."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 1-4, 6-7, 9, 20, and 22-29 are rejected under 35 U.S.C. 102(b) as being anticipated

by Scholl et al. (U.S. Patent Number 5,742,762; hereinafter Scholl).

15. Regarding claim 1, Scholl discloses a method of remotely retrieving the state of at least one

enterprise device, said method comprising:

- providing a reporting and maintenance computer system (Figure 3, Network Management Gateway);

- connecting a superintendent system to the reporting and maintenance computer system (Figure 3, Web Server), said connecting producing a first communications channel (Figure 3, Request and response link);

  ❑ connecting an enterprise to the reporting and maintenance computer system, the

    enterprise including at least one enterprise device that can be enabled to send status

    messages (Figure 3, Managed Network systems 9);

  ❑ receiving enterprise device status requests from the superintendent system at the

    reporting and maintenance computer system (Col 6, lines 9-15);

  ❑ forming responses to enterprise device status requests at the reporting and

    maintenance computer system (Col 6, lines 15-21 and 32-40); and

  ❑ sending the responses from the reporting and maintenance computer system to the

    superintendent system (Col 6, lines 40-41).

16. Regarding claim 20, Scholl discloses a method for determining the state of a remotely

located enterprise, comprising:

  ❑ accessing a reporting and maintenance system (Figure 3, Network Management

    Gateway) (Col 6, lines 6-15),

  ❑ the reporting and maintenance system being operably connected to communicate with

    enterprise devices (Managed Network Elements) in an enterprise (Managed Network)

    (Figure 3).

  ❑ sending a request to the reporting and maintenance system requesting the status of a

    particular enterprise device (Col 6, lines 6-15);

  ❑ receiving a response from the reporting and maintenance system including the status

    of the particular enterprise device (Col 6, lines 32-36); and

  ❑ providing a visual indication of the status of the particular enterprise device (web

    page displayed) (Col 6, lines 37-45).

The following limitations, *having at least two redundant servers, a control unit whereby the power of the servers may be controlled, a cabinet restricting access to the servers, an electronic door lock remotely and locally controllable, two temperature sensors monitoring the temperature of the air inside and outside the cabinet, an alarm, and a camera,* merely restrict the reporting and maintenance system *structure*. However, the reporting and maintenance system *structure* has no bearing on the *method* for determining the state of a remotely located enterprise and is therefore arbitrary. Thus, a prior art rejection which 1) teaches the method steps of the claimed invention and 2) is capable of accessing a reporting maintenance system with the above defined structure, is proper. In the instant case, the system disclosed by Scholl is capable of accessing a reporting maintenance system with the above-defined structure or any other computing device that has a structure capable of communication with other devices.

17. Regarding claims 22 and 26, Scholl discloses a method for remotely accessing and viewing information about an enterprise, comprising the steps of:

- □ accessing a transferential system (Figure 3, Network Management Gateway) (Col 6, lines 6-15);

- □ utilizing the transferential system to access an enterprise (Figure 3, Managed Networks) (Col 6, lines 15-24); and

- □ utilizing the transferential system to view information about the status and operation of the enterprise and its components (viewing the response web page) (Col 6, lines 32-45).

The transferential system characteristics (listed below) merely restrict the transferential system *structure*. However, the transferential system *structure* as claimed has no bearing on the

method for determining the state of a remotely located enterprise and is therefore arbitrary.

Thus, a prior art rejection which 1) teaches the *method* steps of the claimed invention and 2) is

capable of accessing a transferential system with the above defined structure, is proper. In the

instant case, the system disclosed by Scholl is capable of accessing a transferential system with

the structure listed below or any other computing device that has a structure capable of

communication with other devices.

- transferential system characteristics: a server group including at least two servers, said servers providing redundancy of operation, at least one non-volatile memory device incorporated to said server group, server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity, first computer readable instructions installed to said memory devices, said first instructions providing the function of receiving first messages from enterprise devices in at least one enterprise management protocol including version 1 of SNMP, second computer readable instructions installed to said memory devices, said second instructions providing the function of forwarding the information contained in the first messages to a superintendent system by a notification channel in preferential order by an assigned priority, third computer readable instructions installed to said memory devices, said third instructions providing the function of filtering the first

messages, the filtering preventing the forwarding of some of the first messages, said

filtering prescribed by policy, fourth computer readable instructions installed to said

memory devices, said fourth instructions providing the function of assigning priority

to the information in said first messages, fifth computer readable instructions installed

to said memory devices, said instructions providing the function of translating the

first received messages to a second protocol, a cabinet housing said server group, a

first network enabled temperature sensor, said first temperature sensor positioned to

monitor the temperature of the air at the interior of said cabinet, a second network

enabled temperature sensor, said second temperature sensor positioned to monitor the

temperature of the air outside said cabinet, at least one door included in said cabinet

whereby access to said server group is restricted when said doors are in closed

position, locks included in said doors whereby said doors may be secured in a closed

position, said locks enabled to unlock through an electronic command message from

a superintendent system, a data entry device connected to said locks, said data entry

device being mounted to said cabinet, said data entry device providing a human

interface external to the cabinet enclosure; said locks enabled to be unlocked through

said data entry device, a network enabled camera whereby a space in proximity to

said server group may be monitored, an alarm in proximity to said server group, a

network enabled power controller connected to and being configurable to control the

power of at least one server of said server group, said power controller being

configurable to accept network commands from a superintendent system, sixth

computer readable instructions installed to said memory devices, said instructions

providing the function of receiving second messages from a superintendent system through a notification channel, said second messages referencing at least one enterprise device, seventh computer readable instructions installed to said memory devices, said instructions providing the function of translating the second received messages to an enterprise management protocol utilized by the referenced enterprise devices, eighth computer readable instructions installed to said memory devices, said instructions providing the function of forwarding the information in the second messages to the referenced enterprise devices in at least one enterprise management protocol including version 1 of the simple network management protocol, enterprise devices in electronic communication with said server group through said server network hardware, a superintendent system in electronic communication with said server group through said server network hardware, ninth computer readable instructions installed to said memory devices, said ninth instructions providing the function of accepting network parameters that define the boundaries of an enterprise, said ninth instructions also providing the function of discovering enterprise devices through said server network hardware using the network parameters, and tenth computer readable instructions installed to said memory devices, said tenth instructions providing the function of receiving a software upgrade from a superintendent system, said tenth instructions also providing the function of delivering the software upgrade to enterprise devices;

18. Regarding claim 2, Scholl discloses prior to said forming, querying an enterprise device for status; said forming produces a response using the result of said querying (Col 6, lines 15-21 and 32-40).

19. Regarding claim 3, Scholl discloses maintaining a database reflecting the state of enterprise devices (Figure 4, Component 14; Col 7, lines 2-4); said forming produces a response using the database (Col 6, lines 60-65).

20. Regarding claim 4, Scholl discloses periodically polling enterprise devices for status and entering the polled status into the database (Col 7, lines 59-67).

21. Regarding claim 6, Scholl discloses translating communications at the reporting and maintenance computer system between a first protocol and a second protocol, the first protocol being used for communications between the reporting and maintenance computer system and at least one enterprise device, and the second protocol being used for communications between the reporting and maintenance computer system and the superintendent system (Request Col 6, lines 6-8, 15-21 and Response Col 6, lines 32-40).

22. Regarding claim 7, Scholl discloses wherein the first protocol is the SNMP (Col 6, lines 25-26).

23. Regarding claim 9, Scholl discloses the second protocol is a notification channel protocol (HTTP) (Col 6, lines 6-15).

24. Regarding claims 23-25 and 27-29, Scholl discloses using information gained about the enterprise to generate policy or to initiate a physical action. Scholl also discloses using the transferential system to make a modification to the enterprise. (configuration, fault, or performance management) (Col 9, lines 1-13).

25. Claims 11-14, 16-17, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by

Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker).

26. Regarding claim 11, Barker discloses a method of monitoring the state of at least one

enterprise device, said method comprising:

- providing a reporting and maintenance computer system being connectable to said

  enterprise devices (Figure 2, Element Management System Server);

- connecting a superintendent system to the reporting and maintenance computer

  system (Figure 2, Element Management System Client), said connecting producing a

  first communications channel (Figure 2);

- connecting an enterprise to the reporting and maintenance computer system, the

  enterprise including at least one enterprise device (Figure 2, Network Element) that

  can be enabled to send status messages (Traps, Col 11, lines 43-47);

- receiving first enterprise device status messages at the reporting and maintenance

  computer system from the enterprise devices within the enterprise (Col 11, lines 21-

  26);

- filtering the enterprise device status messages using a filter criteria (Col 17, lines 5-

  17); and

- sending second filtered enterprise device status messages from the reporting and

  maintenance system to the superintendent system over the first communications

  channel (Col 17, lines 5-17).

27. Regarding claim 12, Barker discloses said filtering is through policy (Col 17, lines 33-39).

28. Regarding claim 13, Barker discloses the first communications channel is an encrypted

channel (Col 8, lines 45-49).

29. Regarding claim 14, Barker discloses periodically polling enterprise devices for status (Col

4, lines 45-46).

30. Regarding claims 16 and 17, Barker discloses translating first enterprise device status

messages from a first protocol (SNMP) to a second protocol (HTTP); said receiving of second

device status messages receives the first messages in the first protocol; and said sending of

second device status messages uses the product of said translating (Figure 3, see communication

between Element management system client and Element management system server and

Network element, 80).

31. Regarding claim 19, Barker wherein the second protocol is a notification channel protocol

(HTTP) (Figure 3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

32. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scholl et al. (U.S.

Patent Number 5,742,762) and Williams et al. (U.S. Patent Number 6,144,669; hereinafter

Williams).

33. Regarding claim 5, as cited above Scholl discloses receiving responses at the reporting and

maintenance computer system (network management gateway) and sending them out to the

superintendent system (web server) however Scholl fails to disclose categorizing the responses

into at least two priority groups and sending the responses with respect to priority. Nevertheless

it was well known in the art at the time of the invention to assign priority to incoming messages

and then send the received messages out according the their respective priority, as evidenced by

Williams. In a related art, Williams discloses categorizing incoming responses (frames) into

either a high-priority or low priority (Col 9, lines 29-33) queue (Col 9, lines 42-49). Williams

further discloses that the categorized responses are then sent with respect to priority (Col 10,

lines 45-48). It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the system of Scholl to include the priority response categorization and

sending system disclosed by Williams, in order to minimize network instability by facilitating

the delivery of high priority messages (Williams Col 9, lines 14-18).

34. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scholl et al. (U.S.

Patent Number 5,742,762).

35. Regarding claim 8, Scholl fails to disclose using the HTTP protocol for communication

between the reporting and maintenance computer system and at least one enterprise device.

However Scholl does disclose that communication between the reporting and maintenance

computer system and at least one enterprise device occurs using an appropriate protocol for

communication (Col 6, lines 17-20). By using HTTP for communication between the reporting

and maintenance computer system and the superintendent system Scholl discloses HTTP is an

appropriate communication protocol and therefore also appropriate for communication between

the reporting and maintenance computer system and at least one enterprise device. Thus, it

would have been obvious to one of ordinary skill in the art at the time of invention to use the

HTTP protocol from communication between the reporting and maintenance computer system

and at least one enterprise device since Scholl discloses HTTP is an appropriate protocol (Col 6,

lines 6-15).

36. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scholl et al. (U.S.

Patent Number 5,742,762) and Examiner's official notice.

37. Regarding claim 10, Scholl fails to disclose the first communications channel is an

encrypted channel however, the Examiner takes official notice that was well known in the art at

the time of invention to encrypt communications over a network channel. It would have been

obvious to one of ordinary skill in the art at the time of the invention to encrypt communications

between the network management gateway and network management systems of Scholl, so

communication between the devices is secure.

38. Claims 15, 18, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker

et al. (U.S. Patent Number 6,363,421).

39. Regarding claims 15 and 21, Barker discloses a method for managing an enterprise

comprising:

> ❑ assembling an enterprise management system having a central information system
>
>   (Figure 2, Element Management System Client) and an interfacing device whereby an

administrator may interact with the central information system (Figure 2, Element

Management System Client, monitor and input means needed for interaction e.g.

keyboard and/or mounse), such interaction being at least the display of enterprise

device state (Col 1, lines 36-48), the enterprise management system further having a

transferential system enabled to communicate in network fashion with the central

information system and with the enterprise devices of the enterprise (Figure 2,

Element Management System Server);

Barker fails to disclose the transferential system having at least a high priority message

queue (Command Acks and responses) and a low priority message queue (informational

messages) where sending the messages in a preferential order by an assigned priority. However,

Barker does disclose that enterprise devices do. Barker discloses that enterprise devices send

traps to the transferential system in a preferential order by an assigned priority using high and

low priority queues (i.e. command acks being high priority and information messages being low

priority) so the transferential system is not overwhelmed, a form of overload control (Col 34,

lines 51-60). Barker further discloses that client (central information server) overload may be a

problem so overload controls should be implemented to restrict client overload (Col 29, lines 41-

53). Thus, it would have been obvious to one of ordinary skill in the in the art at the time of the

invention to implement the enterprise device overload controls within the transferential system,

in order to prevent the central information server from being overloaded with messages.

In further considering the limitation of claim 21 recited below, such actions are inherent

to priority based sending see Col 34, lines 51-60.

      ❑ testing for the presence of a message in the high priority queue; on condition of

presence of a message in the high priority queue, sending and deleting a message

from the high priority queue; on condition of absence of a message in the high

priority queue, testing for a message in the low priority queue; and on condition of

absence of a message in the high priority queue and presence of a message in the low

priority queue, sending and deleting a message from the low priority queue

40. Regarding claim 18, Scholl fails to disclose using the HTTP protocol for communication

between the reporting and maintenance computer system and at least one enterprise device.

However it was well known in the art at the time of the invention to use the HTTP protocol for

communication between two devices, as evidenced by Barker using HTTP for communication

between the Element Management System Client and the Element Management Server (Figure

3). Therefore, it would have been obvious to one of ordinary skill in the art at the time of

invention to use the HTTP protocol for communication between the reporting and maintenance

computer system and an enterprise device within the Barker system since the HTTP provides an

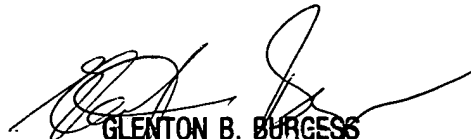efficient means of communication.

Conclusion

41. The prior art made of record, in PTO-892 form, and not relied upon is considered pertinent

to applicant's disclosure.

42. This office action is made **NON-FINAL.**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sean Reilly whose telephone number is 571-272-4228. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

2/25/2005

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100